

**In the Claims**

The following Listing of Claims replaces all prior versions in the application:

## LISTING OF CLAIMS

1-2. (Canceled)

3. (Currently amended) Method set forth in claim 14, characterised in that the keys CW, KR<sub>c</sub> and KP<sub>c</sub> are encrypted by three different service keys, namely K<sub>s</sub>, K<sub>sr</sub> and K<sub>sp</sub> respectively.

4. (Currently amended) Access control method controlling access to a broadcast digital dataflow previously scrambled using an encryption key CW transmitted in encrypted form in an entitlement control message ECM also including at least one access control criterion CA, said numeric data possibly being recorded as such in a receiving terminal or decrypted during transfer, wherein:

on transmission:

- generating an entitlement control message R-ECM<sub>c</sub> for recording the content of the flow as a function of a recording key KR<sub>c</sub> and at least one criterion CRR defining a right to record,

- generating an entitlement control message P-ECM<sub>c</sub> controlling access to play back the content of the recorded flow as a function of a playback key KP<sub>c</sub> and at least one criterion CRP defining a right to play back, and

on reception:

- analyzing the message R-ECM<sub>c</sub>, and

- authorizing the recording if the criterion CRR is verified, otherwise prohibiting recording,

- analyzing the message P-ECM<sub>c</sub>, and

- authorizing the playback if the criterion CRP is verified, otherwise prohibiting the playback,

wherein the keys CW, KR<sub>c</sub> and KP<sub>c</sub> are encrypted by a first service key K<sub>s</sub>,

and wherein for a Method set forth in claim 2, characterised in that the sending phase and

for each dataflow:

- ~~breakdownning the breaking down~~ a scrambling period into a sequence of crypto-periods  $CF_i, CP_i$  each defining a validity duration of an individual key  $CW_i$ , and at each crypto-period change,
- scrambling the content of the flow using the key  $CW_i$ , and ~~memorise~~ memorizing a value  $p(i)$  representative of the parity of  $i$ ,
- ~~calculatinging~~ an entitlement control message ~~SC-ECM<sub>i</sub>SC-ECM<sub>i</sub>~~ SC-ECM<sub>i</sub> as a function of the previously defined encryption keys  $CW_{i-1}$ ,  $CW_i$ ,  $CW_{i+1}$ , the value  $p(i)$  and the criterion  $CA_i$ , said message ~~SC-ECM<sub>i</sub>SC-ECM<sub>i</sub>~~ SC-ECM<sub>i</sub> being intended to transport access rights to a data segment  $S_i$  corresponding to at least two crypto-periods,
- encrypting the keys  $CW_{i-1}$ ,  $CW_i$ ,  $CW_{i+1}$ , using the playback key  $KP_c$ ,
- encrypting the result of the encryption in the previous step using a second service key  $K'_s$ ,
- encrypting the result of the encryption in the previous step using the recording key  $KR_c$ .

5. (Currently Amended) Access control method controlling access to a broadcast digital dataflow previously scrambled using an encryption key CW transmitted in encrypted form in an entitlement control message ECM also including at least one access control criterion CA, said numeric data possibly being recorded as such in a receiving terminal or decrypted during transfer, wherein:

on transmission:

- generating an entitlement control message R-ECM<sub>c</sub> for recording the content of the flow as a function of a recording key KR<sub>c</sub> and at least one criterion CRR defining a right to record,
- generating an entitlement control message P-ECM<sub>c</sub> controlling access to play back the content of the recorded flow as a function of a playback key KP<sub>c</sub> and at least one criterion CRP defining a right to play back, and

on reception:

- analysing the message R-ECM<sub>c</sub>, and
- authorizing the recording if the criterion CRR is verified, otherwise prohibiting recording,
- analyzing the message P-ECM<sub>c</sub>, and

- authorizing the playback if the criterion CRP is verified, otherwise prohibiting the playback,

wherein the keys  $CW$ ,  $KR_C$  and  $KP_C$  are encrypted by a first service key  $K_S$ ,

and wherein for a sending phase and that includes the following steps:

for each dataflow:

- ~~breakdownning the~~ breaking down a scrambling period into a sequence of crypto— periods  $CP_i$  each defining a validity duration of an individual key  $CW_i$ , and at each crypto-period change,

- scrambling the content of the flow using the key  $CW_i$ , and ~~memorise~~ memorizing a value  $p(i)$  representative of the parity of  $i$ ,

- calculating an entitlement control message  $SC-ECM_i$  as a function of the previously defined encryption keys  $CW_{i+1}$ ,  $CW_i$ ,  $CW_{i+1}$ , the value  $p(i)$  and the criterion  $CA_i$ , said message  $SC-ECM_i$  being intended to transport access rights to a data segment  $S_i$  corresponding to at least two crypto-periods,

- encrypting the keys  $CW_{i+1}$ ,  $CW_i$ ,  $CW_{i+1}$  using a second service key  $K'_s$ ,

- encrypting the result of the encryption in the previous step using the key  $KP_C$ ,

- encrypting the result of the encryption in the previous step using the recording key  $KR_C$ .

6. (Previously presented) Method set forth in claim 4, characterised in that the emission phase also includes the following steps:

- calculating the entitlement control message  $ECM_i = f[(ECW_i, OCW_i, CA)]$  wherein  $ECW_i$  and  $OCW_i$  represent the even and odd control words previously encrypted using a first service key  $K_S$ , respectively

$ECW_i = CW_i$  if  $i$  is even, otherwise  $ECW_i = CW_{i+1}$ ;

$OCW_i = CW_i$  if  $i$  is odd, otherwise  $OCW_i = CW_{i+1}$

- broadcasting parameters in the ECM signal, identifying the ECM channels attached to the service broadcasting the content of messages  $ECM_i$ ,  $P-ECM_c$ ,  $R-ECM_c$ ,  $SC-ECM_i$ ,

- providing the  $ECM_i$ ,  $P-ECM_c$ ,  $R-ECM_c$ ,  $SC-ECM_i$  messages to the receiving terminal.

7. (Original) Method set forth in claim 6, characterised in that the  $ECM_i$ ,  $P-ECM_c$ ,  $R-ECM_0$ ,  $SC-ECM_i$  messages are broadcast on ECM channels associated with the content of segment  $S_i$ .

8. (Original) Method set forth in claim 6, characterised in that the R-ECM message is output to the receiving terminal on request from an Authorisation Server at the network entry.

9. (Original) Method set forth in claim 6, characterised in that the P-ECM message is output to the receiving terminal on request from an Authorisation Server at the network entry.

10. (Original) Method set forth in claim 7, characterised in that the reception phase includes the following steps:

- recovering the ECM channel from the  $ECM_i$  message, using the signal attached to the service broadcasting the dataflow, and at each change of  $i$ ,
- analysing the message  $ECM_i$  so as to recover the even control word OCW and the odd control word ECW, to descramble the content of the broadcast flow so as to obtain direct access to this content.

11. (Original) Method set forth in claim 7, characterised in that the reception phase includes the following steps:

- recovering the ECM channel from the  $P-ECM_c$ ,  $R-ECM_c$ ,  $SC-ECM_i$  messages, from the signal attached to the service broadcasting the content;
- analysing the  $R-ECM_c$  message to verify record access criteria CRR,
- memorising the recording key  $KR_c$
- recovering the message  $P-ECM_c$  and store it with the content; and
- for each crypto-period  $i$ :
- recovering the message  $SC-ECM_i$ ,
- decrypting the message  $SC-ECM_i$  using the recording key  $KR_c$ , and
- recording the decrypted message  $SC-ECM_i$  with the content.

12. (Original) Method set forth in claim 7, characterised in that playback access to the content in the recorded flow is obtained according to the following steps:

- recovering the message  $P-ECM_c$  in the content and analyse it to verify read access criteria CRP,
- memorising the playback key  $KP_c$ , and

- recovering the current SC—ECM<sub>i</sub> message in the content;
- decrypting the SC-ECM<sub>i</sub> message with the playback key KP<sub>c</sub> and verify access criteria,
- recovering the encrypted keys CW<sub>i+1</sub>, CW<sub>i</sub>, CW<sub>i+1</sub> and the value p(i) indicating the parity of i, and
- decrypting said keys depending on the read direction to deduce ECW and OCW from them; then
- applying either ECW or OCW to descramble the content when playing back.

13. (Original) Method set forth in claim 7, characterised in that access to play back the content of the flow is obtained according to the following steps:

- recovering the message P-ECM<sub>c</sub> in the content,
- analysing the message P-ECM<sub>c</sub> to verify read access criteria CRP,
- memorising KP<sub>c</sub>, and
- recovering the current SC-ECM<sub>i</sub> message in the content,
- decrypting the SC-ECM<sub>i</sub> message with the second service key K'<sub>s</sub> and verify access criteria,
- recovering the encrypted keys CW<sub>i+1</sub>, CW<sub>i</sub>, CW<sub>i+1</sub> and the value p(i) indicating the parity of i, and
- decrypting said keys depending on the direction of reading to deduce ECW and OCW; then
- applying either ECW or OCW to descramble the content.

14. (Previously presented) Method set forth claim 11, characterised in that the reception phase also includes the following steps:

- generating a local key K<sub>l</sub> from attributes contained in the message R-ECM and at least one parameter related to the identity of the receiving terminal,
- locally over-encrypting the content to be recorded with this key K<sub>l</sub>.
- when playing back, regenerating the key K<sub>l</sub> using attributes contained in the message P-ECM and at least one parameter related to the identity of the receiving

terminal,

- decrypting the recorded content using the 10 regenerated key  $K_I$ .

15. (Currently amended) Access control method controlling access to a broadcast digital dataflow previously scrambled using an encryption key CW transmitted in encrypted form in an entitlement control message ECM also including at least one access control criterion CA, said numeric data possibly being recorded as such in a receiving terminal or decrypted during transfer, wherein:

on transmission:

- generating an entitlement control message R-ECM<sub>c</sub> for recording the content of the flow as a function of a recording key KR<sub>c</sub> and at least one criterion CRR defining a right to record,

- generating an entitlement control message P-ECM<sub>c</sub> controlling access to play back the content of the recorded flow as a function of a playback key KP<sub>c</sub> and at least one criterion CRP defining a right to play back, and

on reception:

- analysing the message R-ECM<sub>c</sub>, and

- authorizing the recording if the criterion CRR is verified, otherwise prohibiting recording,

- analyzing the message P-ECM<sub>c</sub>, and

- authorizing the playback if the criterion CRP is verified, otherwise prohibiting the playback,

~~Method set forth in claim 1, characterised in that~~ wherein the broadcast digital dataflow is of represent-audiovisual programs.

16. (Currently amended) Access control system controlling access to a digital ~~dataflow~~ dataflow including a scrambling platform (2) including at least one generator of entitlement control messages ECM and at least one ~~desrambling~~ descrambling receiver (4) provided with a security processor-(14), characterized in that the scrambling platform (2)-also includes:

- a generator of entitlement control messages R-ECM<sub>c</sub> when recording the content of the received flow and a generator of entitlement control messages P-ECM<sub>c</sub> when playing back the content of a recorded flow, and in that the descrambling receiver-(4),

includes:

- means of recovering the ECM channel from P-ECM<sub>c</sub>, R-ECM<sub>c</sub> messages,
- means of decrypting the content of a received flow to record it, and
- means of decrypting the content of a recorded flow to play it back,
- means for breaking down a scrambling period into a sequence of crypto-periods CP<sub>i</sub> each defining a validity duration of an individual key CW<sub>i</sub>, and at each crypto-period change,
- means for scrambling the content of the flow using a key CW<sub>i</sub>, and memorizing a value p(i) representative of the parity of i,
- calculating an entitlement control message SC-ECM<sub>i</sub> as a function of previously defined encryption keys CW<sub>i-1</sub>, CW<sub>i</sub>, CW<sub>i+1</sub>, the value p(i) and a criterion CA<sub>i</sub>, said message SC-ECM<sub>i</sub> being intended to transport access rights to a data segment S<sub>i</sub> corresponding to at least two crypto-periods,
- encrypting the keys CW<sub>i-1</sub>, CW<sub>i</sub>, CW<sub>i+1</sub>, using the playback key KP<sub>c</sub>,
- encrypting the result of the encryption in the previous step using a second service key K'<sub>s</sub>,
- encrypting the result of the encryption in the previous step using the recording key KR<sub>c</sub>.

17. (Currently amended) System set forth in claim 16, characterised in ~~S~~that that the descrambling receiver (4) also includes means of generating a local key K<sub>l</sub> from attributes contained in the R-ECM<sub>c</sub> message and the identity of the receiving terminal to locally encrypt/decrypt the content of the received flow.

18. (Canceled)

19. (Currently amended) Scrambling platform including at least one generator of entitlement control messages ECM controlling access to a dataflow broadcast in scrambled form, characterised in that it also includes a generator of entitlement control messages R-ECM<sub>c</sub> to control recording the content of a received flow and a generator of entitlement control messages P-ECM<sub>c</sub> to control play back the content of a recorded flow, and further including~~Scrambling platform set forth in claim 18, characterised in that it includes:~~

- means of breaking down the scrambling period into a sequence of crypto-periods  $CP_i$  each defining a validity duration of an individual key  $CW_i$ ,
- means of encrypting the content of the flow at each change of the crypto-period  $i$  using the key  $CW_i$ ,
- means of calculating an entitlement control message  $SC-ECM_i$  as a function of the keys  $CW_{i-1}, CW_i, CW_{i+1}$  corresponding to crypto-periods  $CP_i, CP_{i-1}$  and  $CP_{i+1}$  respectively, a parity parameter  $p(i)$  and the access control criterion  $CA_i$ , said message  $SC-ECM_i$  being intended to carry access rights to a data segment  $\sim 1$  corresponding to at least two crypto-periods,
- means of encrypting the keys  $CW_{i-1}, CW_i, CW_{i+1}$  using a playback key  $KP_c$ ,
- means of encrypting the encryption result in the previous step using a second service key  $K'_s$ ,
- means of encrypting the result of the encryption in the previous step using a record key  $KR_c$ .

20. (Currently amended) Scrambling platform including at least one generator of entitlement control messages ECM controlling access to a dataflow broadcast in scrambled form, characterised in that it also includes a generator of entitlement control messages R-ECM<sub>c</sub> to control recording the content of a received flow and a generator of entitlement control messages P-ECM<sub>c</sub> to control play back the content of a recorded flow~~Platform set forth in claim 18, characterised in that it also includes, and further including:~~

- means of breaking down the scrambling period into a sequence of crypto-periods  $CP_i$  each defining a validity duration of an individual key  $CW_i$ ,
- means of encrypting the content of the flow at each change of the crypto—period  $i$  using the key  $CW_i$ ,
- means of calculating an entitlement control message  $SC-ECM_i$  as a function of the keys  $CW_{i-1}, CW_i, CW_{i+1}$  corresponding to crypto-periods  $CP_i, CP_{i-1}$  and  $CP_{i+1}$  respectively, a parity parameter  $p(i)$  and the access control criterion  $CA_i$ , said message  $SC-ECM_i$  being intended to carry access rights to a data segment  $S_i$  corresponding to at least two crypto-periods,
- means of encrypting the encryption result in the previous step using a second service key  $K'_s$ ,



- means of encrypting the control words  $CW_{i+1}$ ,  $CW_i$ ,  $CW_{i+1}$  using a playback key  $KP_c$ ,
- means of encrypting the encryption result in the previous step using a record key  $KR_c$ .

21. (Currently amended) Descrambling receiver (4) of a dataflow broadcast in scrambled form using a scrambling key  $CW_1$  including a security processor including at least one key  $KR_c$  intended to descramble record entitlement control messages  $R-ECM_c$  and at least one key  $KP_c$  intended to descramble the play back entitlement control messages  $P-ECM_0$ , receiver characterised in that it includes:

- means of recovering the ECM channel from  $P-ECM_c$  messages, and  $R-ECM_c$  messages from the signal attached to the service broadcasting the content;
- means of decrypting messages  $R-ECM_c$  using the record key  $KR_c$  to verify the right to record the content of a received flow,
- means of decrypting messages  $P-ECM_c$  using the key  $KP_c$  to verify the right to play back the content of a recorded flow,
- means for breaking down a scrambling period into a sequence of crypto-periods  $CP_i$  each defining a validity duration of an individual key  $CW_i$ , and at each crypto-period change,
- means for scrambling the content of the flow using a key  $CW_i$ , and memorizing a value  $p(i)$  representative of the parity of  $i$ ,
- calculating an entitlement control message  $SC-ECM_i$  as a function of previously defined encryption keys  $CW_{i-1}$ ,  $CW_i$ ,  $CW_{i+1}$ , the value  $p(i)$  and a criterion  $CA_i$ , said message  $SC-ECM_i$  being intended to transport access rights to a data segment  $S_i$  corresponding to at least two crypto-periods,
- encrypting the keys  $CW_{i-1}$ ,  $CW_i$ ,  $CW_{i+1}$ , using the playback key  $KP_c$ ,
- encrypting the result of the encryption in the previous step using a second service key  $K'_s$ ,
- encrypting the result of the encryption in the previous step using the recording key  $KR_c$ .

22. (Original) Receiver set forth in claim 21, characterized in that it also includes means of generating a local key  $K_l$  from attributes contained in the receiver identity message R-ECM and locally decrypt the content of the received flow.

23. (Original) Receiver set forth in claim 21, characterised in that the security processor is a smart card.

24. (Currently amended) Access control method controlling access to a broadcast digital dataflow previously scrambled using an encryption key CW transmitted in encrypted form in an entitlement control message ECM also including at least one access control criterion CA, said numeric data possibly being recorded as such in a receiving terminal or decrypted during transfer, wherein:

on transmission:

- generating an entitlement control message R-ECM<sub>c</sub> for recording the content of the flow as a function of a recording key KR<sub>c</sub> and at least one criterion CRR defining a right to record,

- generating an entitlement control message P-ECM<sub>c</sub> controlling access to play back the content of the recorded flow as a function of a playback key KP<sub>c</sub> and at least one criterion CRP defining a right to play back, and

on reception:

- analysing the message R-ECM<sub>c</sub>, and

- authorizing the recording if the criterion CRR is verified, otherwise prohibiting recording,

- analyzing the message P-ECM<sub>c</sub>, and

- authorizing the playback if the criterion CRP is verified, otherwise prohibiting the playback,

wherein the keys CW, KR<sub>c</sub> and KP<sub>c</sub> are encrypted by three different service keys, namely K<sub>s</sub>, K<sub>sf</sub> and K<sub>sp</sub> respectively, and

wherein for a Method set forth claim 3, characterised in that the sending phase and for includes the following steps:

for each dataflow:

- ~~breakdownning~~ breaking down a the scrambling period into a sequence of crypto-

periods  $CF_i$  each defining a validity duration of an individual key  $CW_i$ , and at each crypto— period change,

- scrambling the content of the flow using the key  $CW_i$ , and memorise a value  $p(i)$  representative of the parity of  $i$ ,ing an entitlement control message  $SC\text{---}ECM_i$  as a function of the previously defined encryption keys  $CW_{i-1}$ ,  $CW_i$ ,  $CW_{i+1}$ , the value  $p(i)$  and the criterion  $CA_i$ , said message  $SC\text{---}ECM_i$  being intended to transport access rights to a data segment  $S_i$  corresponding to at least two crypto-periods,

- encrypting the keys  $CW_{i-1}$ ,  $CW_i$ ,  $CW_{i+1}$ , using the playback key  $KP_c$ ,

- encrypting the result of the encryption in the previous step using a second service key  $K'_s$ ,

- encrypting the result of the encryption in the previous step using the recording key  $KR_c$ .

25. (Currently amended) Access control method controlling access to a broadcast digital dataflow previously scrambled using an encryption key  $CW$  transmitted in encrypted form in an entitlement control message  $ECM$  also including at least one access control criterion  $CA$ , said numeric data possibly being recorded as such in a receiving terminal or decrypted during transfer, wherein:

on transmission:

- generating an entitlement control message  $R\text{---}ECM_c$  for recording the content of the flow as a function of a recording key  $KR_c$  and at least one criterion  $CRR$  defining a right to record,

- generating an entitlement control message  $P\text{---}ECM_c$  controlling access to play back the content of the recorded flow as a function of a playback key  $KP_c$  and at least one criterion  $CRP$  defining a right to play back, and

on reception:

- analysing the message  $R\text{---}ECM_c$ , and

- authorizing the recording if the criterion  $CRR$  is verified, otherwise prohibiting recording,

- analyzing the message  $P\text{---}ECM_c$ , and

- authorizing the playback if the criterion  $CRP$  is verified, otherwise prohibiting the playback,

wherein the keys  $CW$ ,  $KR_c$  and  $KP_c$  are encrypted by three different service keys, namely  $K_s$ ,  $K_{sr}$  and  $K_{sp}$  respectively, and wherein for a Method set forth claim 3, characterised in that the sending phase includes the following steps:and

for each dataflow:

- ~~breakdownning~~ breaking down the scrambling period into a sequence of crypto—periods  $CP_i$  each defining a validity duration of an individual key  $CW_i$ , and at each crypto-period change,
  - scrambling the content of the flow using the key  $CW_i$ , and memorise a value  $p(i)$  representative of the parity of  $i$ ,
  - calculating an entitlement control message SC-  $ECM_i$  as a function of the previously defined encryption keys  $CW_{i+1}$ ,  $CW_i$ ,  $CW_{i+1}$ , the value  $p(i)$  and the criterion  $CA_i$ , said message SC- $ECM_i$  being intended to transport access rights to a data segment  $\sim 1$  corresponding to at least two crypto-periods,
  - encrypting the keys  $CW_{i+1}$ ,  $CW_i$ ,  $CW_{i+1}$  using a second service key  $K'_s$ ,
  - encrypting the result of the encryption in the previous step using the key  $KP_c$ ,
  - encrypting the result of the encryption in the previous step using the recording key  $KR_c$ .

26. (Previously presented) Method set forth claim 5, characterised in that the emission phase also includes the following steps:

- calculating the entitlement control message  $ECM_i = f[(ECW_i, OCW_i, CA)]$  wherein  $ECW_i$  and  $OCW_i$  represent the even and odd control words previously encrypted using a first service key  $K_s$ , respectively

$ECW_i = CW_i$  if  $i$  is even, otherwise  $ECW_i = CW_{i+1}$ ;

$OCW_i = CW_i$  if  $i$  is odd, otherwise  $OCW_i = CW_{i+1}$

- broadcasting parameters in the ECM signal, identifying the ECM channels attached to the service broadcasting the content of messages  $ECM_i$ , P- $ECM_c$ , R-  $ECM_c$ , SC- $ECM_i$ ,
- providing the  $ECM_i$ , P- $ECM_c$ , R- $ECM_c$ , SC- $ECM_i$  messages to the receiving terminal.

27. (Previously presented) Method set forth claim 12, characterised in that the reception phase also includes the following steps:

- generating a local key  $K_l$  from attributes contained in the message R-ECM and at least one parameter related to the identity of the

receiving terminal,

- locally over-encrypting the content to be recorded with this key  $K_I$ .
- when playing back, regenerating the key  $K_I$  using attributes contained in the message P-ECM and at least one parameter related to the identity of the receiving terminal,
- decrypting the recorded content using the 10 regenerated key  $K_I$ .